Föderiertes Identity Management

10. Tagung der DFN-Nutzergruppe Hochschulverwaltung

Berlin, 09.05.-11.05.2011

Peter Gietz, CEO, DAASI International GmbH

Peter.gietz@daasi.de

DAASI International GmbH

Agenda

1) Begriffe Identity Management und Federated Identity Management
2) Motivation für Föderiertes Identity Management in der Hochschulverwaltung
3) Der Standard SAML
4) Open Source Implementierung Shibboleth
5) Wege einer Hochschule zu Föderiertem Identity Management

DAASI International GmbH

1) Begriffe
Identity Management
und
Federated Identity Management

Identity Management

- **Definition von Spencer C. Lee:**
  - ***Identity Management bezieht sich auf den Prozess der Implementierung neuer Technologien zum Verwalten von Informationen über die Identität von Nutzern und zur Kontrolle des Zugriffs auf Firmenressourcen.***
  - ***Das Ziel von Identity Management ist es Produktivität und Sicherheit zu erhöhen und gleichzeitig Kosten der Verwaltung von Benutzern, ihrer Identitäten, Attribute und Berechtigungsnachweise zu senken***
- **Im Kontext Federated Identity Management:**
  - **Identity Management ist Voraussetzung für Federated Identity Management da Zusagen über Aktualität und Richtigkeit der Identitätsdaten gemacht werden**

DAASI International GmbH

Federated Identity Management

- *FIdM-Definition von Peter Valkenburg, et.al (SURF):*
  - *Kollektiver Begriff für alle Prozesse, Standards und Technologien, die den Austausch von Identitäts-informationen über organisatorische Grenzen hinweg unterstützen*
- **FidM setzt eine Föderation voraus**
  - **Ein Vertrauensbund, der es ermöglicht, verteilte Ressourcen gemeinsam zu nutzen**
  - **Vertrauen wird durch Verträge und Einhaltung von entsprechenden Sicherheitspolicies gewährleistet**

DAASI International GmbH

Grundbausteine einer Föderation

- Eine Föderation besteht aus drei Bausteinen:
  - Föderationsverwaltung
    - zentraler Vertragspartner für Föderationsmitglieder
    - verwaltet Zugangsdaten zu den einzelenen Bausteinen (“Metadaten”)
    - betreibt zentrale Infrastrukturkomponenten
  - Identity Provider (IdP)
    - Benutzerverwaltung der Heimatorganisation
    - verantwortlich für Authentifizierung und Attribute
  - Service Provider (SP)
    - verantwortlich für Ressourcen
    - Entscheidet aufgrund von Aussagen des IdP

DAASI International GmbH

Vorteile von FIdM

- Identitätsdaten eines Benutzers müssen nur an einer Stelle gespeichert werden
  - Name, Kontaktdaten, Passwort, etc.
  - im IdP der „Heimatorganisation“
- Personenbezogene Daten
  - werden nur über gesicherte Verbindungen an Mitglieder des Vertrauensbunds geschickt
  - müssen aber gar nicht übertragen werden, da es nur auf Autorisierungsattribute ankommt
- Die Föderationstechnologien ermöglichen Single Sign On
- Föderation ähnelt einer PKI (Public Key Infrastructure), ist aber wesentlich einfacher zu implementieren:
  - nur Serverzertifikate notwendig
  - Passwort anstelle der Benutzerzertifikate

DAASI International GmbH

2) Motivation für Federated Identity Management in der öffentlichen Verwaltung

DAASI International GmbH

Motivation im Hochschulbereich

- **Hochschulen waren und sind wichtige Treiber für FidM, überall mit ähnlichen Motiven:**
  - **Studenten werden immer mobiler, wechseln die Hochschule öfters, bzw. belegen Kurse an anderen Hochschulen (E-Learning)**
  - **Forschung funktioniert immer vernetzter**
    - **Forscher aus verschiedenen Hochschulen benötigen Zugriff auf im Netz verteilte Ressourcen („Virtuelle Organisationen“)**
    - **eScience und Grid-Computing**
    - **Auch Cloud-Computing stellt ähnliche Anforderungen**
  - **Verlagslizenzen erfordern Föderationen**
    - **z.B. für Datenbanken, die von Hochschulbibliotheken online gestellt werden**
    - **Verlage wollen Autorisierungsattribute (anstelle von IP-Ranges)**
    - **Lizenzen können auch an Hochschulverbünde erteilt werden**

DAASI International GmbH

Neue Interessenten im Behördenkontext

- Viele Behörden sind dezentral organisiert, wollen aber zentrale Dienste anbieten, z.B.:
  - Bundesbehörden mit vielen Dienststellen im gesamten Bundesgebiet
  - Kultusministerien, die für alle Schulen Dienste anbieten
  - Alle Behörden eines Ministeriums
  - Behörden verschiedener Ministerien, die auf gleiche Anwendungen zugreifen
- In all diesen Fällen können die Benutzerdaten in der Heimatbehörde bzw. Heimatorganisation Schule bleiben
- Auch hier scheinen sich die selben Technologien, die im Hochschulbereich verwendet werden, durchzusetzen

DAASI International GmbH

Motivation Single Sign On

- Technologien für Föderiertes Identitäts-Management bieten sozusagen als „Nebennutzen“ Single Sign On für Webanwendungen:
  - Nicht nur hat man nur einen Account/Passwort für alle Anwendungen
  - man muss sich auch pro Tag nur einmal authentifizieren
- Für viele Projekte ist dieser „Nebennutzen“ der wichtigste Treiber
  - Es gibt viele Organisation, die diese Technologien ohne Beitritt zu einer Föderation verwenden

DAASI International GmbH

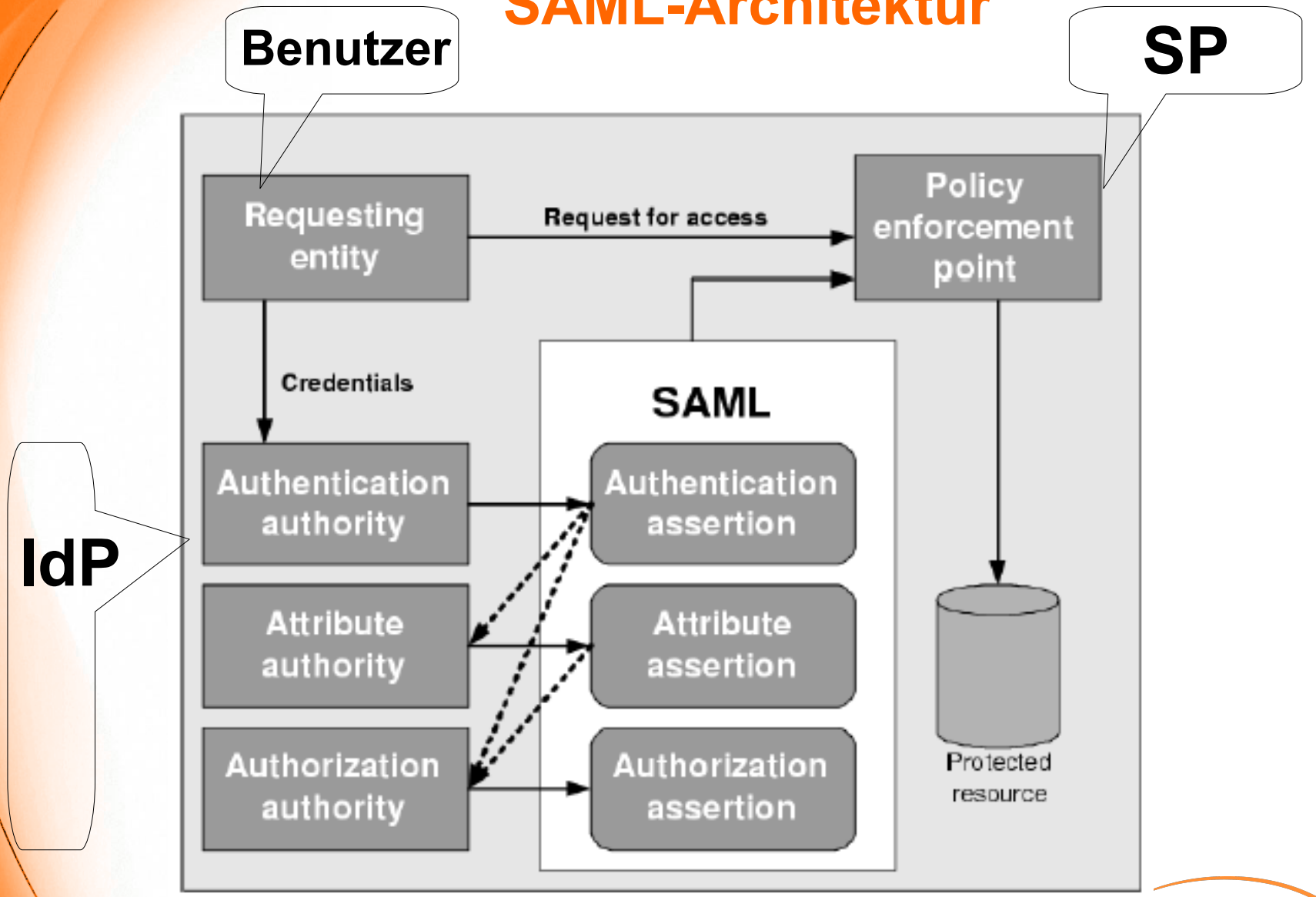
3) Der Standard SAML

SAML

- Security Assertion Markup Language
  - OASIS-Standard
- XML-Dokumente enthalten Zusicherungen (Assertions) die ein IdP über Benutzer macht:
  - Authentication Statements, Zusicherung, dass sich ein Benutzer authentifiziert hat
  - Authorization Statement, Zusicherung über bestimmte Zugriffsrechte
  - Attribute Statement, Zusicherung über bestimmte Eigenschaften eines Benutzers, die in Form von Attributen weitergegeben werden und den SP bei der Entscheidung über Zugriff unterstützen
- Profile spezifizieren welche Assertions wie zwischen IdP und SP ausgetauscht werden

DAASI International GmbH

SAML-Architektur

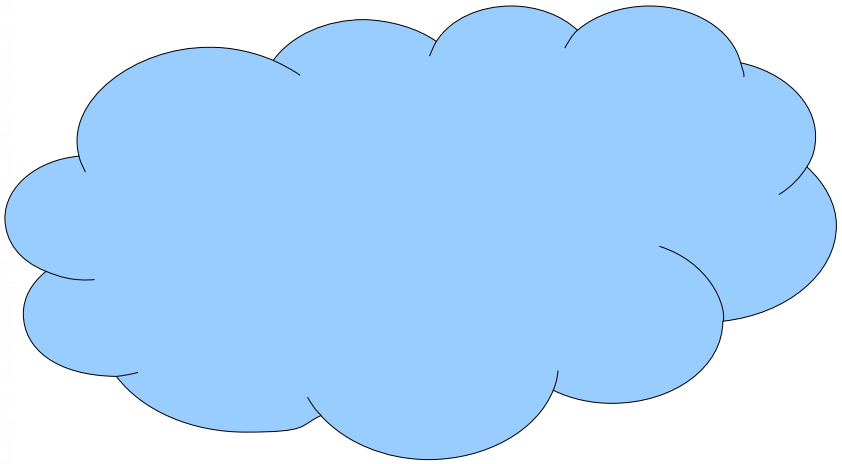


Nach: RUBENKING, NEIL J.: Securing web services

DAASI International GmbH

SAML hat sich etabliert

- SAML hat sich als Standard durchgesetzt
- Wird neuerdings auch von Microsoft unterstützt nachdem vergeblich versucht wurde, eigene Standards zu setzen
- SAML löst auch AAI-Probleme des Cloud-Computing, weshalb ich eine wolkige Zukunft sehe



DAASI International GmbH

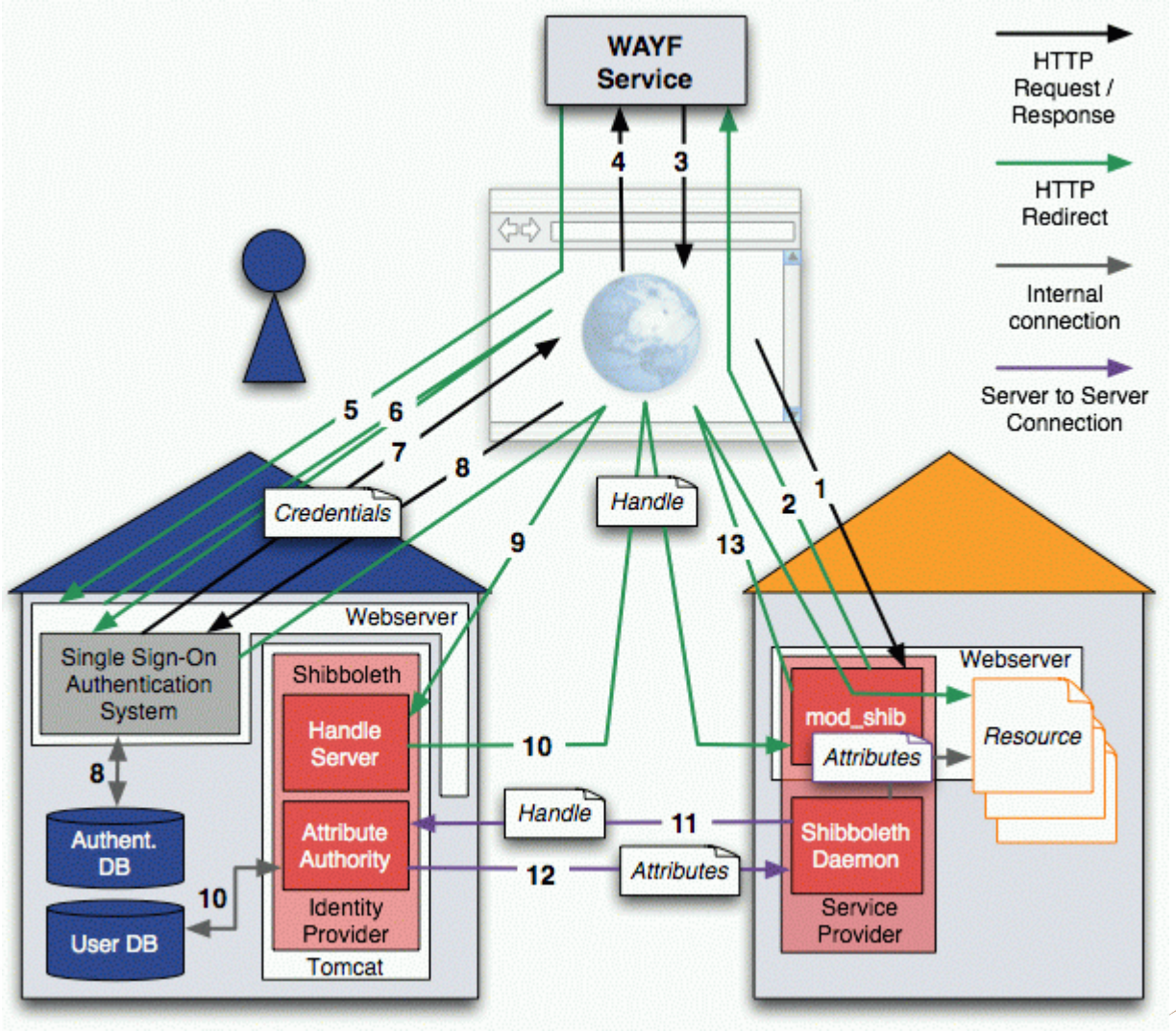
4) Open Source Implementierung Shibboleth

Shibboleth

- Open Source Software vom US-amerikanischen Internet2-Projekt
- Implementiert das SAML-Profil WebSSO
  - nach einmaliger Authentifizierung hat der Nutzer für eine bestimmte Zeit föderationsweit Zugriff auf verschiedene Webanwendungen
- Viele Anwendungen sind bereits „shibboletisiert“
- Shibboleth baut im Wesentlichen auf zwei miteinander kommunizierende (Apache-)Module auf:
  - Identity Provider (IdP), der an die lokalen Benutzerverwaltungen angeschlossen wird
  - Service Provider (SP), der vor zu schützende Ressourcen bzw. Dienste gestellt wird.

DAASI International GmbH

Shibboleth Architektur



DAASI International GmbH

5) Wege einer Hochschule zu Föderiertem Identity Management

Voraussetzungen für Föderiertes IdM

- **Wichtigste Voraussetzung ist die Implementierung eines Identity Management Systems:**
  - **Einrichtung einer möglichst alle wichtigen Bereiche abdeckende Task-Force zur Planung und Umsetzung**
    - **Hochschulleitung, Hochschulverwaltung, CIO, Bibliothek, Rechenzentrum, Datenschützer, Personalrat, Fakultäten**
  - **Schaffung einer Übersicht über alle zentral nutzbaren Infrastrukturen und Anwendungen, sowie weiterer Anforderungen (Compliance, Auditing, etc.)**
  - **Feinkonzept, Datenschutzanalyse, Implementoerungsplan**
  - **Aufbau der technischen Komponenten**
    - **Zentraler Verzeichnisdienst (LDAP), Konnektoren zu Quelldatenbanken, Provisionierungsschnittstellen zu anzuschließenden Systemen, Auditing-Komponenten, etc.**

DAASI International GmbH

Weitere Schritte hin zu Föderierten IdM

- Der LDAP-Server muss mit Föderationsrelevanten Attributen gefüllt werden
  - EduPerson, TERENA SCHAC, sowie für eLearning dfnPerson
  - Dies kann schon bei der Einführung von IdM berücksichtigt werden
- Planung:
  - welche Komponenten sollen an die Föderation angeschlossen werden?
  - Welche Webanwendungen sollen in das SSO-System integriert werden?
- Aufbau der technischen Komponenten
  - Identity Provider vor dem LDAP-Server
  - Service-Provider vor den Webanwendungen

DAASI International GmbH

Anschluss an die DFN-AAI

- Anmelden der Komponenten an die DFN-AAI-Testföderation
- Evaluation, der verschiedenen Sicherheitsstufen der DFN-Föderation
- Unterschreiben der Föderationsverträge
  - mindestens für den IdP
  - Wenn Sie Ihre Dienste der Föderation zur Verfügung stellen wollen (z.B. e-Learning-Angebote) auch für einen oder mehrere SPs
- Anmelden der Komponenten an der Produktiv-DFN-AAI

DAASI International GmbH

Vielen Dank für Ihre Aufmerksamkeit!

Fragen ?

- Kontakt und weitere Informationen:
  - DAASI International GmbH
    Europaplatz 3
    D-72072 Tübingen

    Web: http://www.daasi.de
    Mail: info@daasi.de

  - Bei späteren Fragen zum Vortrag:
    Mail: peter.gietz@daasi.de

DAASI International GmbH